CVSS

The Common Vulnerability Scoring System

April 13, 2004
NIAC Vulnerability Disclosure Working Group
Scoring Subgroup

John Chambers
President & CEO
Cisco Systems, Inc.

John Thompson
Chairman & CEO
Symantec Corp.

Agenda

- Background
- Scope
- Status
- CVSS Framework
- Next Steps
- Timeline

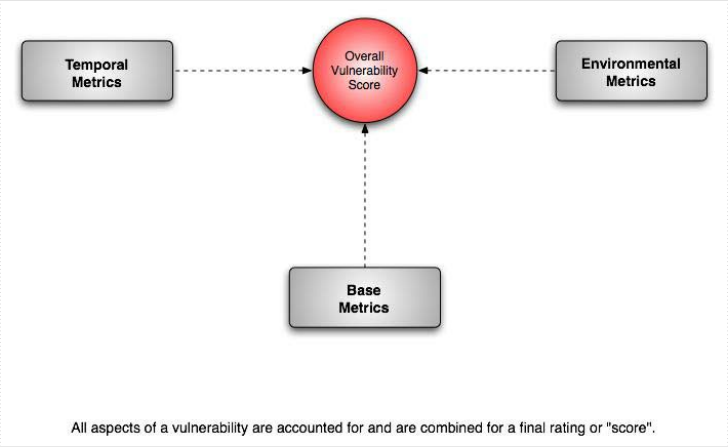
Background

- Vulnerability Disclosure WG determined need for common scoring methodology in Jul 2003
- NIAC tasked Scoring Subgroup Oct 2003
- Purpose: Develop common vulnerability scoring methodology to promote understanding of severity, risk, and potential impact to aid in prioritizing response actions

Scope

- "Common Vulnerability Scoring System (CVSS)"
  - Provides a way to evaluate vulnerabilities with a composite score representing overall severity and risk presented by a vulnerability
- Modular Approach
  - Promotes consistency; easy to use
  - Accounts for time-dependent properties
  - Adaptable for different environments
- Does not address disclosure issues
  - Refer to NIAC disclosure guidelines

Proposed Common Vulnerability Scoring System



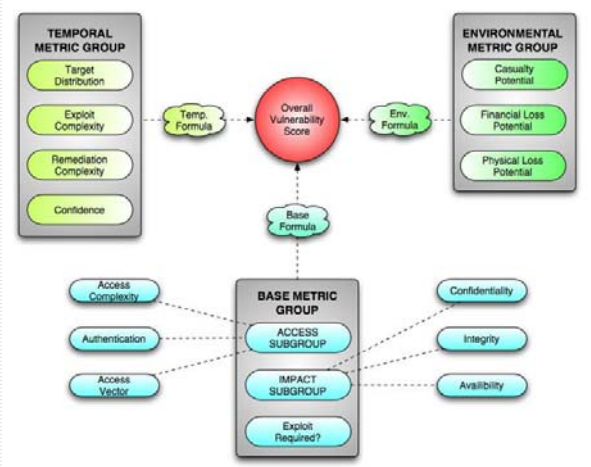
April 2004 Status

- 75% complete
  - Components, formulas drafted
  - Standard process developed
- Planning real-world testing
  - Dry runs using selected vulnerabilities
  - Adding additional industry participation in study groups for validation

Metrics

- A constituent component or characteristic of a vulnerability that can be quantitatively or qualitatively measured
- Three classes:
  - Base Metrics
  - Temporal Metrics
  - Environmental Metrics
- CVSS uses a total of 14 different metrics

CVSS with Metrics



Base Metrics

- Intrinsic and fundamental qualities of a vulnerability
- Do not change over time
- Do not change in different environments

Temporal Metrics

- Time-dependent characteristics
- Allow for change as the vulnerability ages

Environmental Metrics

- Characteristics that are tied to implementation and environment
- Can be different for different stakeholders

Scoring and Formulas

- Each metric is weighted and combined according to specific formulas
- One formula for each group
  - Base formula
  - Temporal formula
  - Environmental formula
- End result is a single score

Next Steps

- Testing:
  - Test with selected vulnerabilities
  - Validate with industry study groups
- Take feedback from testing and improve system
- Complete report to NIAC
- Propose draft standard
- Pending NIAC approval and industry acceptance, submit IETF draft

Timeline

- June 1, 2004: Complete real-world testing
- June 15, 2004: Complete validation
- June 30, 2004: Complete feedback and finalize CVSS
- June 30, 2004: Complete report for NIAC
- July 30, 2004: Draft proposed standard

Discussion

- Questions?